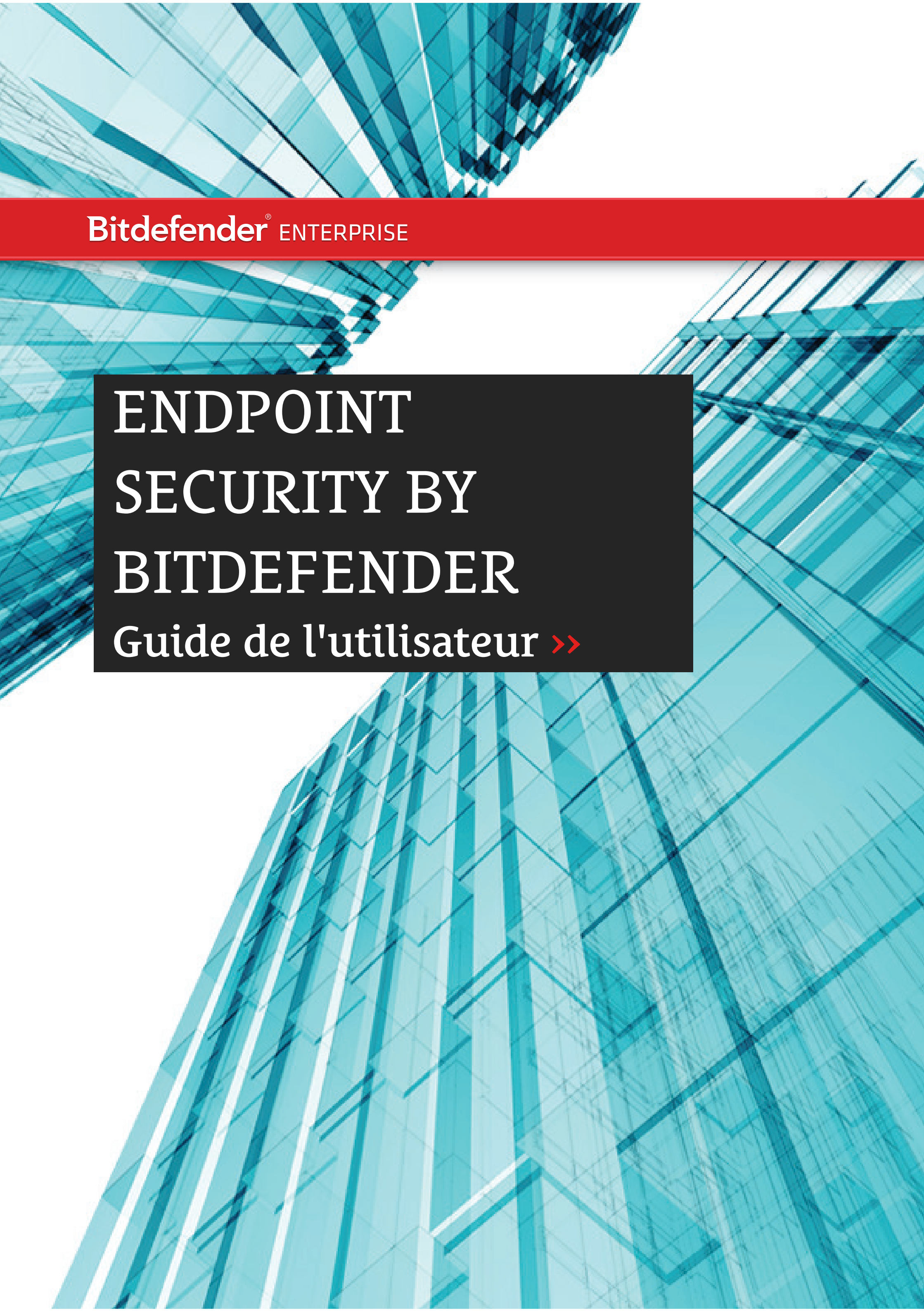

Bitdefender® ENTERPRISE
ENDPOINT SECURITY BY BITDEFENDER
Guide de l'utilisateur ››

Date de publication 2014.09.30


Bitdefender®

Table des matières

Utilisation de ce guide

1. Objectifs et destinataires

Cette documentation est conçue pour les utilisateurs finaux d'**Endpoint Security**, le logiciel client Security for Endpoints installé sur les ordinateurs et les serveurs pour les protéger contre les malwares et les autres menaces Internet et pour appliquer les politiques de contrôle utilisateur.

Les informations présentées ici devraient être faciles à comprendre pour toute personne capable de travailler sous Windows.

Nous vous souhaitons un apprentissage agréable et utile.

2. Comment utiliser ce guide

Ce guide est organisé afin de trouver facilement les informations dont vous avez besoin.

« Pour démarrer » (p. 1)
Découvrez l'interface utilisateur de Endpoint Security.

« Analyse antimalware » (p. 9)
Découvrez comment exécuter des analyses antimalwares.

« Mises à jour » (p. 17)
En savoir plus sur les mises à jour de Endpoint Security.

« Événements » (p. 19)
Vérifiez l'activité de Endpoint Security.

« Obtenir de l'aide » (p. 20)
Sachez où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

3. Conventions utilisées dans ce guide

Normes Typographiques

Plusieurs styles de texte sont utilisés dans ce guide pour une meilleure lisibilité. Leur aspect et signification sont présentés dans le tableau ci-dessous.

Apparence	Description
documentation@bitdefender.com	Les adresses e-mail sont insérées dans le texte pour plus d'informations sur les contacts.
« Utilisation de ce guide » (p. v)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
`nom de fichier`	Les fichiers et répertoires sont imprimés en utilisant des caractères `séparés d'un espace`.
option	Toutes les options du produit sont imprimées à l'aide de caractères **gras**.
mot clé	Les mots-clés et les expressions importantes sont mises en évidence à l'aide de caractères **gras**.

Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.



Note

La note consiste simplement en une courte observation. Bien que vous puissiez les ignorer, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien vers un thème proche.



Important

Cette icône requiert votre attention et il n'est pas recommandé de la passer. Elle fournit généralement des informations non essentielles mais importantes.

4. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons fait notre possible pour tester et vérifier toutes les informations. N'hésitez pas à nous écrire pour nous signaler des erreurs dans ce livret ou concernant toute amélioration que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Faites le nous savoir en nous écrivant à cette adresse documentation@bitdefender.com. Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.

1. Pour démarrer

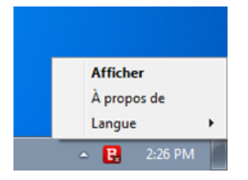
Endpoint Security est un programme de sécurité informatique entièrement automatisé, administré à distance par votre administrateur réseau. Une fois installé, il vous protège contre toutes sortes de malwares (virus, spywares et chevaux de Troie), attaques du réseau, phishing et vol de données. Il peut également être utilisé pour appliquer les politiques d'utilisation d'Internet et des ordinateurs de votre entreprise.

Endpoint Security prendra pour vous la plupart des décisions de sécurité et affichera rarement des alertes pop-up. Des détails sur les actions prises et des informations sur le fonctionnement du programme sont disponibles dans la fenêtre Événements. Pour plus d'informations, reportez-vous à « Événements » (p. 19).

1.1. Icône de la zone de notification

Lors de l'installation, Endpoint Security place une icône dans la zone de notification. Si vous double-cliquez sur cette icône, la fenêtre principale du programme s'affichera. Si vous faites un clic droit sur l'icône, un menu contextuel vous fournira des options utiles.

- **Afficher** - ouvre la fenêtre principale de Endpoint Security.
- **À propos de** - ouvre une fenêtre contenant des informations relatives à Endpoint Security, ainsi que des éléments d'aide si vous rencontrez une situation anormale. Ouvrir cette fenêtre lance automatiquement une mise à jour à la demande.
- **Langue** - vous permet de changer la langue de l'interface utilisateur.



Icône de la zone de notification

L'icône Endpoint Security de la zone de notification vous signale la présence de problèmes affectant votre ordinateur en modifiant son apparence :

Des problèmes critiques affectent la sécurité de votre système.

Des problèmes non critiques affectent la sécurité de votre système.



Note

L'administrateur réseau peut choisir de masquer l'icône de la zone de notification.

1.2. Ouverture de la fenêtre principale du programme

Pour accéder à l'interface principale d'Endpoint Security, utilisez le menu Démarrer de Windows en suivant le chemin **Démarrer** → **Programmes** → **Endpoint Security by Bitdefender** → **Ouvrir la Console de Sécurité** ou double-cliquez directement sur l'icône de Endpoint Security B dans la zone de notification.

1.3. Fenêtre principale du programme

La fenêtre principale d'Endpoint Security vous permet de consulter l'état de la protection et d'effectuer des tâches d'analyse. Tout se trouve à quelques clics. La configuration et l'administration de la protection est réalisée à distance par votre administrateur réseau.

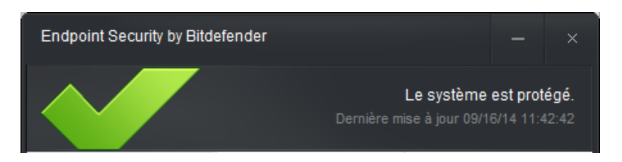


Fenêtre principale du programme

La fenêtre est organisée en deux zones principales :

Zone de notification

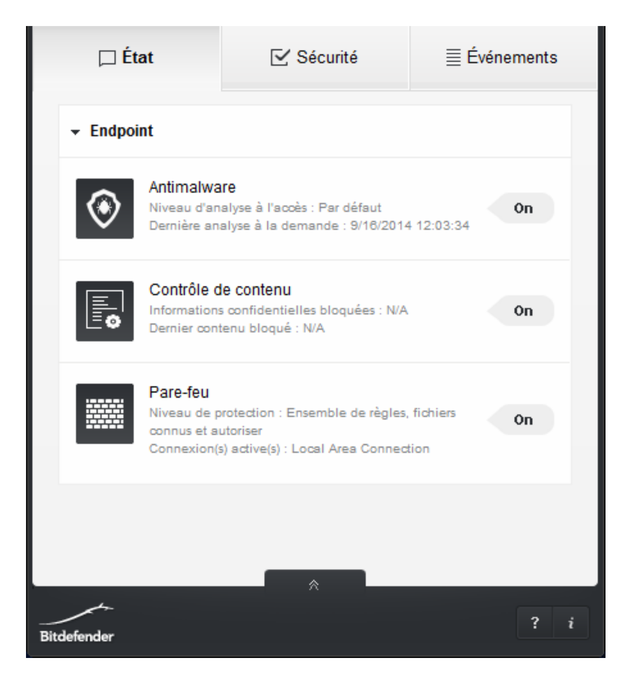
Vous pouvez consulter ici l'état de sécurité de votre ordinateur et voir les problèmes affectant la sécurité de votre système.



Zone de notification

Panneaux

Les panneaux vous permettent de connaître l'état de tous les modules de protection installés, de gérer les tâches d'analyse à la demande et de voir les événements enregistrés par Endpoint Security.



Panneaux

Vous trouverez également des options de support utiles dans la partie inférieure de la fenêtre :

Option	Description
?	Cliquez sur cette icône si vous avez besoin d'aide avec Endpoint Security.
i	Cliquez sur cette icône pour des informations sur le produit et de contact.

1.3.1. Zone de notification

La zone de notification fournit des informations utiles au sujet de la sécurité du système.

Vous pouvez identifier facilement l'état de sécurité actuel grâce au symbole d'état qui apparaît à gauche de la zone de notification :

- **Un symbole vert.** Il n'y a pas de problèmes à corriger. Votre ordinateur et vos données sont protégés.
- **Un point d'exclamation jaune.** Des problèmes non critiques affectent la sécurité de votre système.
- **Un point d'exclamation rouge.** Des problèmes critiques affectent la sécurité de votre système.

En plus du symbole d'état, un message d'état de sécurité détaillé s'affiche à droite de la zone de notification. Vous pouvez voir les problèmes de sécurité détectés en cliquant sur la zone de notification. Les problèmes existants seront corrigés par votre administrateur réseau.

1.3.2. Panneaux

Les panneaux vous permettent de connaître l'état de tous les modules de protection installés, de gérer les tâches d'analyse à la demande et de voir les événements enregistrés par Endpoint Security.

Les panneaux disponibles dans cette zone sont :

État

Vous y trouverez des informations utiles au sujet de l'état et de l'activité des modules de protection installés.

- **Antimalware.** La protection antimalware est la base de votre sécurité. Endpoint Security vous protège en temps réel et à la demande contre toutes sortes de malwares tels que les virus, les chevaux de Troie, les spywares, les adwares etc.
- **Contrôle de contenu.** Le module Contrôle de contenu vous protège lorsque vous êtes sur Internet contre les attaques de phishing, les tentatives de fraude, la divulgation de données personnelles et le contenu web inapproprié. Il comprend également un ensemble complet de contrôles utilisateur qui aident l'administrateur réseau à appliquer les politiques d'utilisation des ordinateurs et d'Internet.

- **Mise à jour.** Le module de mise à jour garantit que Endpoint Security et les signatures de virus sont mises à jour.
- **Pare-feu.** Le pare-feu vous protège lorsque vous êtes connecté à des réseaux et à Internet en filtrant les tentatives de connexion et en bloquant les connexions suspectes ou risquées.
- **Général.** La catégorie Général fournit tous les détails qui ne sont pas couverts par les modules mentionnés ci-dessus, tels que les informations sur les licences du produit.

Sécurité

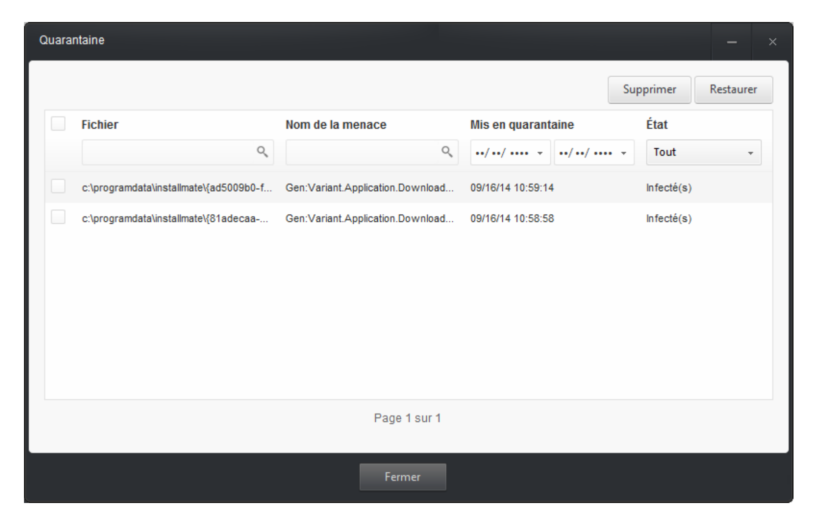
Vous pouvez lancer ici les analyses du système. Vous pouvez exécuter l'une des tâches d'analyse suivantes :

- **Quick Scan** utilise l'analyse in-the-cloud pour détecter les malwares présents sur votre système. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.
- L'**Analyse Complète** analyse l'ensemble de votre ordinateur afin de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.
- **Analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.

Pour plus d'informations, reportez-vous à « Analyse antimalware » (p. 9).

Sous la section **Quarantaine**, vous pouvez vérifier rapidement combien de fichier ont été placé en quarantaine pendant les tâches d'analyse.

- Pour voir et agir sur les fichiers en quarantaine, cliquez sur le bouton **Voir**. La page **Quarantaine** s'affichera. Vous pouvez voir ici la liste des fichiers en quarantaine, leur chemin d'origine, la date et l'heure de leur mise en quarantaine et leur état de sécurité. Utilisez le bouton en haut à droite afin de supprimer et de restaurer le fichier désiré.



Quarantaine

- Si vous désirez supprimer tous les fichiers de la quarantaine, cliquez sur le bouton **Vider**.

Événements

Cette section vous permet d'accéder à un historique détaillé des événements importants survenus lors de l'activité du produit. Pour plus d'informations, reportez-vous à « Événements » (p. 19).

1.4. Protection navigation web

Votre administrateur de Security for Endpoints peut configurer des paramètres de sécurité ayant un impact sur votre navigation web. Ces paramètres de sécurité peuvent concerner :

- « Barre d'outils Bitdefender » (p. 6)
- « Search Advisor » (p. 7)
- « Pages Web bloquées » (p. 7)

1.4.1. Barre d'outils Bitdefender

Lorsque cela est configuré par votre administrateur de Security for Endpoints, la barre d'outils de Bitdefender vous indique les évaluations de la sécurité des pages web que vous consultez. La barre d'outils de Bitdefender n'est pas votre barre d'outils de navigateur typique. La seule

chose qu'il ajoute au navigateur est un petit bouton en haut de chaque page web. Cliquer sur le bouton ouvre la barre d'outils.

En fonction de la façon dont Bitdefender classifie la page web, l'un des messages suivants s'affiche dans la barre d'outils :

- « Cette page n'est pas sûre » apparaît à côté d'un point d'exclamation rouge.
- « Nous vous recommandons d'être vigilant » apparaît à côté d'un point d'exclamation jaune.
- « Cette page est sûre » apparaît à côté du symbole vert.

1.4.2. Search Advisor

Quand il est installé par l'administrateur Security for Endpoints, Search Advisor évalue les résultats des recherches Google, Bing et Yahoo! ainsi que tous les liens Facebook et Twitter en plaçant une icône devant chaque résultat. Icônes utilisées et leur signification :

Nous vous déconseillons de consulter cette page web.

Cette page web peut contenir du contenu dangereux. Soyez prudent si vous décidez de le consulter.

Cette page n'a pas pu être vérifiée par Endpoint Security.

Cette page peut être consultée en toute sécurité.

1.4.3. Pages Web bloquées

Selon les politiques de sécurité mises en place par votre administrateur Security for Endpoints, des paramètres de sécurité spécifiques au navigateur web contre les fraudes Internet et le phishing peuvent être mis en place. Security for Endpoints peut bloquer automatiquement les pages web de phishing (usurpation de sites web/spoofing) connues afin d'empêcher que les utilisateurs ne divulguent par inadvertance des informations privées ou confidentielles à des fraudeurs en ligne. Outre l'usurpation de sites web, d'autres types de fraudes sur Internet peuvent être bloquées comme : les fraudes d'achats, les arnaques promettant de s'enrichir rapidement, les fraudes de marketing sur Internet, les fraudes au clic, etc. Au lieu de la page web malveillante, une page d'avertissement spéciale s'affiche dans le navigateur afin de vous informer que la page web requise est dangereuse.



Note
Si vous avez besoin d'accéder à une page Web légitime qui est détectée et bloquée à tort, merci de contacter votre administrateur Security for Endpoints pour qu'il puisse mettre en place une dérogation.

1.5. Analyse des périphériques

Endpoint Security peut être configuré pour détecter automatiquement les dispositifs de stockage (CD/DVD, supports de stockage USB, lecteurs mappés du réseau) et vous proposer de les analyser. La fenêtre d'alerte vous fournit des informations sur le périphérique détecté.

Pour analyser le périphérique, cliquez sur **Oui**. Si vous êtes sûr(e) que le périphérique est sain, vous pouvez décider de ne pas l'analyser.



Note
Si plusieurs périphériques sont détectés en même temps, des fenêtres d'alerte s'affichent, l'une après l'autre, pour chacun d'entre eux.

Votre administrateur Security for Endpoints peut choisir de supprimer les alertes et les fenêtres pop-up Endpoint Security. Dans certains cas, l'analyse du périphérique se lance automatiquement, sans que vous n'ayez à vous en occuper.

Lorsque l'analyse d'un périphérique est en cours, une icône de progression de l'analyse apparaît dans la zone de notification. Vous pouvez double-cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement. Vous pouvez suspendre ou arrêter l'analyse du périphérique à tout moment. Pour plus d'informations, reportez-vous à « Assistant d'analyse antivirus » (p. 13).

1.6. Modifier les paramètres de protection

Endpoint Security est configuré et administré à distance par votre administrateur réseau. Vous ne pouvez pas modifier les paramètres de protection.

Si vous avez des questions concernant vos paramètres de protection, veuillez les poser à la personne chargée de la sécurité de votre réseau.

2. Analyse antimalware

Le principal objectif d'Endpoint Security est de maintenir votre ordinateur sans malwares. Il y parvient principalement en analysant en temps réel les fichiers à l'accès, les e-mails et tout nouveau fichier téléchargé ou copié sur votre ordinateur. Outre la protection en temps réel, il permet également d'exécuter des analyses pour détecter et supprimer les malwares de votre ordinateur.

Vous pouvez analyser l'ordinateur quand vous le souhaitez en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser. Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée.

2.1. Analyser un fichier ou un dossier

Il est conseillé d'analyser les fichiers et les dossiers chaque fois que vous soupçonnez qu'ils peuvent être infectés. Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et sélectionnez **Analyser avec Endpoint Security by Bitdefender**. L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

2.2. Exécuter une Analyse Rapide

Quick Scan utilise l'analyse 'in-the-cloud' pour détecter les malwares présents sur votre système. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

Pour effectuer une analyse rapide, suivez ces étapes :

1. Ouvrez la fenêtre Endpoint Security.
2. Allez dans le panneau **Sécurité**.
3. Cliquez sur le bouton **Analyser** correspondant à l'option **Analyse rapide**.
4. Attendez que l'Assistant d'analyse antivirus termine l'analyse. Endpoint Security appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

2.3. Exécuter une Analyse Complète du Système

La tâche d'Analyse Complète du Système analyse l'ensemble de votre ordinateur en vue de détecter tous les types de logiciels malveillants menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.



Note
L'Analyse Complète du système effectuant une analyse approfondie de l'ensemble du système, elle peut prendre quelque temps. Il est donc recommandé d'exécuter cette tâche lorsque vous n'utilisez pas votre ordinateur.

Si vous souhaitez analyser certains emplacements de votre ordinateur ou configurer les options d'analyse, configurez et exécutez une analyse personnalisée. Pour plus d'informations, reportez-vous à « Configurer et exécuter une analyse personnalisée » (p. 10).

Avant d'exécuter une Analyse Complète du Système, nous vous recommandons ceci :

- Vérifiez qu'Endpoint Security dispose de signatures de malwares à jour. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher Endpoint Security de détecter de nouveaux malwares identifiés depuis la précédente mise à jour. Pour plus d'informations, reportez-vous à « Mises à jour » (p. 17).
- Fermez tous les programmes ouverts.

Pour exécuter une Analyse Complète du Système, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Security.
2. Allez dans le panneau **Sécurité**.
3. Cliquez sur le bouton **Analyser** correspondant à l'option **Analyse complète**.
4. Attendez que l'Assistant d'analyse antivirus termine l'analyse. Endpoint Security appliquera automatiquement les actions recommandées aux fichiers détectés. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

2.4. Configurer et exécuter une analyse personnalisée

Pour configurer une analyse antimalware en détail et l'exécuter, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Security.
2. Allez dans le panneau **Sécurité**.
3. Cliquez sur le bouton **Nouveau** correspondant à l'option **Analyse personnalisée**.

   Une nouvelle fenêtre s'affiche. Suivez ces étapes :

a. Vous pouvez facilement configurer les options d'analyse en réglant le niveau d'analyse. Déplacez le curseur sur l'échelle pour choisir le niveau d'analyse souhaité. Reportez-vous à la description à droite de l'échelle pour identifier le niveau d'analyse le plus adapté à vos besoins.

   Les utilisateurs avancés peuvent profiter des paramètres d'analyse proposés par Endpoint Security. Pour configurer les options d'analyse en détail, cliquez sur **Configuration**. Après avoir sélectionné les paramètres personnalisés souhaités, le niveau d'analyse sera automatiquement réglé sur **Personnalisé**. Vous trouverez des informations sur les paramètres personnalisés à la fin de cette section.

b. Vous pouvez aussi configurer ces options générales :

   - **Exécuter la tâche en priorité basse .** Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
   - **Réduire l'assistant d'analyse dans la zone de notification .** Réduit la fenêtre d'analyse dans la zone de notification. Double-cliquez sur l'icône de l'avancement de l'analyse pour l'ouvrir.

4. Cliquez sur **Suivant** pour sélectionner les emplacements à analyser.
5. Cliquez sur le bouton **Ajouter** pour sélectionner les emplacements à analyser. Si vous souhaitez effacer la liste des emplacements cibles, cliquez sur le bouton **Supprimer**.
6. Cliquez sur **Suivant** pour lancer l'analyse et attendez que l'Assistant d'analyse antivirus termine l'analyse. En fonction des emplacements à analyser, l'analyse peut prendre quelque temps. À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.

Informations sur les options d'analyse

Ces informations peuvent vous être utiles :

- Si vous n'êtes pas familiarisé avec certains des termes, consultez le glossaire. Vous pouvez également rechercher des informations sur Internet.
- **Types de fichiers.** Vous pouvez régler Endpoint Security pour analyser tous les types de fichiers ou uniquement les applications (fichiers programmes). L'analyse de tous les fichiers consultés offre une protection maximale, alors que l'analyse des applications offre uniquement une analyse rapide.

  Les applications (ou les fichiers de programmes) sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Cette catégorie comprend les extensions de fichiers suivantes : `386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm;`

dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Options d'analyse pour les archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité de votre système. Les malwares peuvent affecter votre système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.



Note
L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser les secteurs d'amorçage.** Vous pouvez paramétrer Endpoint Security pour qu'il analyse les secteurs d'amorçage de votre disque dur. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus de boot. Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
- **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des rootkits et des objets masqués à l'aide de ce logiciel.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire de votre système.
- **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le Registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.
- **Analyser les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur votre ordinateur.

- **Analyser uniquement les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les keyloggers commerciaux.** Sélectionnez cette option si vous avez installé et utilisez un keylogger commercial sur votre ordinateur. Les keyloggers commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.

2.5. Assistant d'analyse antivirus

À chaque fois que vous lancerez une analyse à la demande (par exemple en faisant un clic droit sur un dossier et en sélectionnant **Analyser avec Endpoint Security by Bitdefender**), l'assistant de l'analyse antivirus d'Endpoint Security s'affichera. Suivez l'assistant pour terminer le processus d'analyse.



Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond. Recherchez l'icône de l'avancement de l'analyse dans la zone de notification. Vous pouvez double-cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

2.5.1. Étape 1 - Effectuer l'analyse

Endpoint Security commencera à analyser les objets sélectionnés. Vous pouvez voir des informations en temps réel sur l'état et les statistiques de l'analyse (y compris le temps écoulé, une estimation du temps restant et le nombre de menaces détectées). Pour plus d'informations, cliquez sur le lien **Plus de statistiques**.

Patientez jusqu'à la fin de l'analyse. L'analyse peut durer un certain temps, suivant sa complexité.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Annuler**. Vous vous retrouverez alors à la dernière étape de l'assistant. Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Archives protégées par mot de passe. Lorsqu'une archive protégée par mot de passe est détectée, en fonction des paramètres de l'analyse, on peut vous demander d'indiquer son mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. Voici les options proposées :

- **Mot de passe.** Si vous souhaitez que Endpoint Security analyse l'archive, sélectionnez cette option et entrez le mot de passe. Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.

- **Ne pas demander le mot de passe et ne pas analyser cet objet.** Sélectionnez cette option pour ne pas analyser cette archive.
- **Ne pas analyser les éléments protégés par mot de passe.** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe. Endpoint Security ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Sélectionnez l'option souhaitée et cliquez sur **OK** pour poursuivre l'analyse.

2.5.2. Étape 2 - Sélectionner des actions

À la fin de l'analyse, on vous demandera de sélectionner les actions à appliquer aux fichiers détectés, le cas échéant.



Note

Si vous lancez une analyse rapide ou une analyse complète du système, Endpoint Security appliquera automatiquement les actions recommandées aux fichiers détectés pendant l'analyse. Si des menaces non résolues sont toujours présentes, on vous demandera de choisir les actions à leur appliquer.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés. Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes. Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Action automatique

Endpoint Security appliquera les actions recommandées en fonction du type de fichier détecté :

- **Fichiers infectés .** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender. Endpoint Security tentera de supprimer automatiquement le code malveillant du fichier infecté et de reconstituer le fichier d'origine. Cette opération est appelée désinfection.

  Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

  Important

  Pour certains types de malware, la désinfection n’est pas possible car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Fichiers suspects.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible. Ils seront placés en quarantaine afin d'éviter une infection potentielle.

  Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Archives contenant des fichiers infectés.**
  - Les archives contenant uniquement des fichiers infectés sont automatiquement supprimées.
  - Si une archive contient à la fois des fichiers infectés et des fichiers sains, Endpoint Security tentera de supprimer les fichiers infectés s'il peut reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Supprimer

Supprime du disque les fichiers détectés.

Si des fichiers infectés sont contenus dans une archive avec des fichiers sains, Endpoint Security tentera de supprimer les fichiers infectés et de reconstituer l'archive avec les fichiers sains. Si la reconstitution de l'archive n'est pas possible, vous serez informé qu'aucune action n'a été appliquée afin d'éviter de perdre des fichiers sains.

Ignorer

Aucune action ne sera menée sur les fichiers détectés. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

2.5.3. Étape 3 - Récapitulatif

Une fois que les problèmes de sécurité auront été corrigés par Endpoint Security, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre. Si vous souhaitez consulter des informations complètes sur le processus d'analyse, cliquez sur **Afficher journal** pour afficher le journal d'analyse.

Cliquez sur **Fermer** pour fermer la fenêtre.



Important

Dans la plupart des cas, Endpoint Security désinfecte les fichiers infectés qu'il détecte ou isole l'infection. Il y a toutefois des problèmes qui ne peuvent pas être résolus automatiquement. Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.

2.6. Consulter les Journaux d'Analyse

À chaque fois que vous effectuez une analyse, un journal d'analyse est créé. Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises à l'encontre de ces menaces.

Vous pouvez ouvrir le journal d'analyse directement à partir de l'assistant d'analyse, une fois l'analyse terminée, en cliquant sur **Afficher le Journal**.

Pour consulter les journaux d'analyse ultérieurement, suivez ces étapes :

1. Ouvrez la fenêtre Endpoint Security.
2. Allez dans le panneau **Événements**.
3. Sélectionnez **Antimalware** dans le deuxième menu. Cette section vous permet de trouver tous les événements d'analyse antimalware, y compris les menaces détectées par l'analyse à l'accès, les analyses lancées par un utilisateur et les modifications d'état pour les analyses automatiques.
4. Dans la liste des événements, vous pouvez consulter les analyses ayant été réalisées récemment. Cliquez sur un événement pour afficher des informations à son sujet.
5. Pour ouvrir le journal d'analyse, cliquez à l'endroit mentionné dans la zone détails en bas du panneau. Le journal d'analyse s'affichera.

3. Mises à jour

Dans un monde où les cybercriminels recherchent sans cesse de nouveaux moyens de nuire, il est essentiel de maintenir sa solution de sécurité à jour afin de conserver une longueur d'avance sur eux.

Si vous êtes connecté à Internet par câble ou DSL,Endpoint Security s'en occupera automatiquement. Par défaut, des mises à jour sont recherchées au démarrage de votre ordinateur puis toutes les **heures** après cela. Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.



Note

La fréquence des mises à jour automatiques par défaut peut être modifiée par votre administrateur réseau. Pour plus d'informations, reportez-vous à « Qu'est-ce que la fréquence de mise à jour automatique ? » (p. 18).

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour Bitdefender à la demande. Pour plus d'informations, reportez-vous à « Mise à jour en cours » (p. 18).

3.1. Types de mise à jour

La section Mise à jour de ce Manuel d'utilisation contient les thèmes suivants:

- **Mises à jour des signatures de malwares** - avec l'apparition de nouvelles menaces, les fichiers contenant des signatures de malwares doivent être mis à jour pour garantir une protection permanente, actualisée.
- **Mise à jour du produit** - quand une nouvelle version du produit est mise en circulation, elle contient de nouvelles fonctionnalités et techniques d'analyse, introduites dans le but d'améliorer les performances du logiciel.

  La mise à niveau d'un produit est une version release principale.

3.2. Vérifier que votre protection est à jour

Pour vérifier que votre protection est à jour, procédez comme suit :

1. Faites un clic droit sur l'icône de Endpoint Security dans la zone de notification et sélectionnez **À propos de**.
2. Vous pouvez voir l'état de la mise à jour et l'heure de la dernière recherche et installation de mise à jour.

Pour des informations détaillées sur les dernières mises à jour, vérifiez les événements de mise à jour :

1. Dans la fenêtre principale, allez dans le panneau **Événements**.
2. Cliquez sur **Mise à jour** dans le deuxième menu.

Vous pouvez savoir quand des mises à jour ont été lancées et obtenir des informations à leur sujet (si elles ont été ou non réussies, si elles nécessitent un redémarrage pour que leur installation se termine). Si nécessaire, redémarrez le système dès que possible.

3.3. Mise à jour en cours

Pour effectuer des mises à jour, une connexion à Internet est requise.

Pour lancer une mise à jour, faites un clic droit sur l'icône de Endpoint Security dans la zone de notification et sélectionnez **À propos de**. Ouvrir la fenêtre **À propos de** lance automatiquement une mise à jour à la demande.

Le module de Mise à jour se connectera au serveur de mise à jour de Bitdefender et recherchera des mises à jour. Si une mise à jour est détectée, elle est automatiquement téléchargée et installée sur votre ordinateur.



Important

Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Il est recommandé de le faire dès que possible

3.4. Qu'est-ce que la fréquence de mise à jour automatique ?

Endpoint Security recherche automatiquement des mises à jour au démarrage de votre ordinateur puis toutes les **heures**.

4. Événements

Endpoint Security tient un journal détaillé des événements concernant son activité sur votre ordinateur (comprenant également les activités surveillées par le Contrôle de contenu). Les événements sont un outil très important pour la surveillance de votre protection Bitdefender. Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc.

Pour consulter le journal des événements, procédez comme suit :

1. Ouvrez la fenêtre Endpoint Security.
2. Allez dans le panneau **Événements**.
3. Sélectionnez la catégorie d'événement dans le second menu. Les événements sont regroupés dans les catégories suivantes :
   - **Antimalware**
   - **Contrôle de contenu**
   - **Mise à jour**
   - **Pare-feu**
   - **Général**

Une liste d'événements est disponible pour chaque catégorie. Pour des informations sur un événement de la liste, cliquez dessus. Des détails sur l'événement s'affichent alors dans la partie inférieure de la fenêtre. Chaque événement est accompagné des informations suivantes : une brève description, l'action que Bitdefender a appliquée et la date et l'heure de l'événement.

Vous pouvez filtrer les événements en fonction de leur importance. Il existe trois types d'événements :

Les événements **Informations** indiquent des opérations réussies.

Les événements **Avertissement** signalent des problèmes non critiques.

Les événements **critiques** signalent des problèmes critiques.

Les événements peuvent uniquement être supprimés par votre administrateur réseau.

5. Obtenir de l'aide

Pour des problèmes ou des questions concernant Endpoint Security, veuillez contacter votre administrateur réseau.

Pour des informations sur le produit et de contact, exécutez l'une des actions suivantes :

- Ouvrez la fenêtre Endpoint Security et cliquez sur l'icône **Infos** dans le coin inférieur droit.
- Faites un clic droit sur l'icône de Endpoint Security dans la zone de notification et sélectionnez **À propos de**.

Glossaire

Adware

Les adwares sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces adwares étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant, les « pop up » publicitaires peuvent devenir contrariants et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Antivirus storm

Utilisation intensive des ressources système se produisant lorsque le logiciel antivirus analyse simultanément plusieurs machines virtuelles sur un seule hôte physique.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Code malveillant

« Malware » est un terme générique regroupant les logiciels conçus pour faire du tort ; il s'agit de la contraction de « malicious software » (logiciels malveillants) L'emploi de ce terme n'est pas encore universel, mais sa popularité pour désigner les virus, les chevaux de Troie, les vers et les codes mobiles malveillants progresse.

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant

pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme le manque de mémoire.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains anciens OS n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)

Fichier qui enregistre les actions ayant eu lieu. La Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Hameçonnage

Action d’envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d’obtenir frauduleusement des informations privées qui permettront d’utiliser l’identité du destinataire de l'e-mail. Cet e-mail oriente l’utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n’a pour objectif que de voler les informations de l’utilisateur.

Heuristique

Méthode basée sur des règles permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros de sécurité sociale).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Logiciel espion

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels sharewares ou freewares pouvant être téléchargés sur Internet. Notons toutefois que la plupart des applications sharewares ou freewares ne comportent pas de spywares. Une fois installé, le spyware surveille l’activité de l’utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même, les numéros de cartes bancaires.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu’un autre produit. Une des manières les plus classiques d'être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d’éthique et de respect de la vie privée, les spywares volent les ressources de l’ordinateur de l’utilisateur en utilisant sa bande passante lors de l’envoi d’informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu’à entraîner des plantages ou provoquer une instabilité globale du système.

Mise à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l’utilisateur de rechercher manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être un virus et ne génère donc pas de fausses alertes.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des logs et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot

Secteur au début de chaque disque qui identifie l’architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge le système d'exploitation.

Signature du malware

Les signatures de malwares sont des fragments de codes extraits à partir de malwares réels. Elles sont utilisées par les programmes antivirus pour rechercher certaines caractéristiques et détecter les malwares. Les signatures sont également utilisées pour supprimer le code malveillant des fichiers infectés.
La base de données de signatures de malwares de Bitdefender rassemble des signatures de malwares mises à jour toutes les heures par les chercheurs de malwares de Bitdefender.

Spam

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des emails non sollicités.

TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier

très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus de boot

Virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Virus polymorphique

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils sont plus difficiles à identifier.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l’horloge) et contient des icônes miniatures permettant d’accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.